CS70 Discussion 2d Review

Agnibho Roy

Summer 2020

1 Review

These are just concepts and strategies discussed during discussion section on July 2, 2020. For definitions and formulas, refer to note 7 on the course website.

1.1 Modular Arithmetic

- Modular Arithmetic is a way for us to look at computation in a specific range of integers from 0 to $m-1$ if we are looking in the modular space m.
- The term $x \equiv r \pmod{m}$ means nothing but, if we take some number x and divide by m, then we will get the remainder r. A common way to move from the modular to the non-modular world is by the representation of the previous equation as $x = qm + r$ for some $q \in Z$.
- Product rule of modular arithmetic (very good for simplifying computation): $a * b \pmod{m} = a \pmod{m} * b \pmod{m}$. The same works for addition as well.
- gcd algorithm: $\gcd(x, y) = \gcd(y, x \pmod{y})$.
- There exists no division in modular arithmetic as we would describe it in the real world, but rather a multiplicative inverse, which is defined as some b for which $a * b = 1 \pmod{m}$. This exists if and only if $\gcd(a, m) = 1$. The inverse can be iteratively guessed or calculated by the egcd algorithm.

2 Extra Problems

These problems are not necessarily in scope. Some may be helpful on exams, but some others are just fun exercises. Reach out to me by email (agnibhoroy@berkeley.edu) if you see any mistakes or have questions about any of the questions.

2.1 Simplify

Simplify the following to a value $0 \leq x < m$ for expressions in modulo m

1. $7^{2020} (\text{mod } 50)$
2. $1! + 2! + 3! \ldots 200! (\text{mod } 24)$

2.2 Fall 2018 Modular Question

Let a sequence of psuedo-random numbers be $x_1, x_2, \ldots x_n$ and the sequence is recursively defined as $x_n \equiv ax_{n-1}$ Here p is a prime number, a is a positive integer such that $a \not\equiv 0 (\text{mod} p)$, and $x_0 \in Z^+$ is a seed (initialization) satisfying $x_0, a \not\equiv 0 (\text{mod} p)$. The period d is the smallest $n \in Z^+$ such that $x_n \equiv x_0 (\text{mod} p)$; note that the sequence repeats after d numbers have been generated. We want to make d as large as possible.

1. for $n \in N$, find x_n as a function of $n, a, \text{and} x_0$.
2. Prove that $a^d \equiv 1 (\text{mod } p)$
3. Let n_0 be the smallest positive integer n such that $a^d \equiv 1 (\text{mod } p)$. Prove that n_0 divides all positive integers n such that $a^n \equiv 1 (\text{mod } p)$.
4. Finally prove that the period d divides $p - 1$. State clearly which results you used to prove this claim.